

REMARKS

This response is submitted in reply to the Office Action dated August 23, 2006. No new matter is added.

35 USC § 112 Rejections

The Office Action rejects Claims 1, 5, 13, 14, 21, 22 and 23 under 35 USC § 112 as failing to comply with the written description requirement and not being described in the specification. Specifically, the Office Action states that “Applicant’s disclosure fails to recite ‘an additional authentication request sent from the information processing apparatus and wherein the additional authentication request is sent only if the decrypted result corresponds to the first data item, and wherein, only when the user has been authenticated in response to the additional authentication request, the authentication apparatus performs processing.’” Applicants respectfully disagree and traverse such rejection.

Applicants respectfully submit that the Claim language is fully supported in the specification. For example, see the specification on page 3 lines 8-13 stating, “... including a step of authenticating the user by the common-key encryption method by using the common key held by the data holding apparatus of the user in response to a user authentication request; and a step of, only when the user has been authenticated, performing processing for authenticating the user by the public-key encryption method.” As further supported in the specification, see also, FIG. 7 where between steps SP 5 and SP 6 the process determines whether or not to send a second authentication request and after authentication, the user is sent a digital signature. Additionally, see the specification on page 3 lines 22-25 stating that after authentication by the common-key encryption method the system performs the step of, “... only when the user has been authenticated in the authentication step, performing processing for making the information processing apparatus authenticate the user by the public-key encryption method by using the private key corresponding to the user.” For at least the foregoing reasons, Applicants respectfully submit that the rejection pursuant to 35 USC § 112 should be withdrawn.

35 USC § 103(a) Rejections

The Office Action rejects Claims 1-23 under 35 USC § 103(a) as being unpatentable over Audebert (US Patent No. 6,694,436). Applicants respectfully disagree and traverse such rejections. The Office Action states that Audebert discloses a user authentication system that, “only when the user has been authenticated, in response to the additional authentication request the authentication apparatus performs processing using the private key corresponding to the user for making the information processing apparatus authenticate the user.” Applicants respectfully disagree and submit that Audebert does not teach, suggest or disclose the element.

Audebert in column 26, lines 37-45 states “[t]his authentication can be effected by a means of conventional challenge/response type mechanism, for example, using a secret shared between the card and the terminal module and symmetrical cryptography or, as already described, using a private key stored by the card enabling the challenge to be encrypted using an asymmetrical algorithm, the terminal module verifying the response using its public key (emphasis added).” Audebert in column 21 line 45 to column 22 line 20 is directed to a system using a PIN for a first authentication step, using a common key system for a second authentication step then retrieval of the private key for digital signature. Audebert is not directed towards using a common key system for a first step of authentication, using the private key of the user to further authenticate the user, then using the private key for further data encryption as is embodied by the claimed invention and fully supported by the specification. Therefore, Applicants respectfully submit that Audebert does not teach, suggest or disclose the subject matter as defined in independent Claims 1, 5, 13, 14, and 21-23, and the Claims that depend therefrom based on at least these reasons.

Additionally, Applicants respectfully submit that Claims 1-23 are patentably distinguishable from the cited art for the reasons above and at least in addition to the further reasons described below. The Office Action states, “[a]lthough steps are not explicitly disclosed with the exact orders claimed, it would only require routine skill in the art to write the steps of the claimed invention using encryption and authentication methods exchanged between the authentication apparatus, the holding medium, and information processing apparatus and the suggestions disclosed by Audebert.” Applicants respectfully disagree and submit that it would not be obvious to one skilled in the art to write the steps of the claimed invention based on Audebert.

A particular advantage is obtained through the use of the common key encryption system for a first step of authentication followed by using public key encryption for a second step of authentication. For example, see the specification on page 3 lines 1-5 stating, “[a]ccording to this authentication system, user authentication is performed with safety provided by the public-key encryption method and quickness provided by the common-key encryption method.” The common key encryption method provides distinct advantages, and the public-key encryption method provides separate distinct advantages.

Further, both encryption systems are used in separate instances, for example see the specification on page 1 lines 18-21 stating, “[s]ince the common-key encryption method performs encryption and decryption within a short period, it is used in cases where information which requires high-speed processing is processed, such as electronic money or commuter-pass information stored in an IC card.” See also, the specification on page 1 lines 24-28 stating in part that the public-key encryption method, “is used in cases where anonymity is required, such as a case in which a financial transaction is achieved on a network such as the Internet.” The two encryption systems are used for different purposes. Therefore, for at least the foregoing reasons, Applicants submit that it would not be obvious to one skilled in the art to arrange the steps of Audebert to achieve the claimed invention.

Accordingly, Applicants believe that the obviousness rejection should be withdrawn and further respectfully submit that the present application is in condition for allowance.

The Commissioner is hereby authorized to charge deposit account 02-1818 for any fees which are due and owing.

Respectfully submitted,

BELL, BOYD & LLOYD LLC

BY 

Thomas C. Basso
Reg. No. 46,541
Customer No. 29175

Dated: October 26, 2006